VAWKUM Transactions on Computer Sciences
http://vfast.org/journals/index.php/VTCS@ 2025, ISSN(e): 2308-8168, ISSN(p): 2411-6335
Volume 13, Number 1, January-June 2025 *pp: 01-19*

5G and AI: Addressing Security Challenges in Next-Generation Wireless Networks Through Machine Learning and Cryptographic Solutions

Abdul Waheed[1*], **Saeed Azfar**[2], **Nadia Mustaqim Ansari**[3], **Rizwan Iqbal**[4], **Maqsood ur Rehman Awan**[5]

[1]MS Cybersecurity, Tandon School of Engineering, New York University; [2]Institute of business Management, Karachi; [3]Department of Electronic Engineering, Dawood University of Engineering and Technology, Karachi; [4]Department of Telecommunication Engineering, Dawood University of Engineering and Technology, Karachi; [5]Department of Electronic Engineering, Dawood University of Engineering and Technology, Karachi

Keywords: *5G security, artificial intelligence, machine learning, cryptographic solutions, post-quantum cryptography, blockchain authentication, anomaly detection, intrusion prevention, network slicing, wireless communication security.*

Journal Info:
Submitted:
February 23, 2025
Accepted:
March 9, 2025
Published:
March 19, 2025

Abstract Modern wireless communication technologies are progressing very fast making it possible to deploy fifth-generation (5G) networks that have high speed with low delay and great connectivity. However, these innovative technologies also bring significant security risks as these are based on distributed environments, network slicing, and software-defined networking. Considering these threats, this research aims to examine the application of artificial intelligence and cryptographic approaches towards mitigating these risks. The use of AI in security has been highlighted to be one of the best security features of current computer and network systems, especially in the case of machine learning. The Convolutional Neural Network (CNN) based detection models like GANs and Auto encoders show good detection rates but have issues of high computational load and energy consumption. Reinforcement learning models provide clients with adaptive solutions for security to change their approach as threats change. Moreover, five advanced solutions include post-quantum cryptography, homomorphic encryption, and blockchain-based authentication to enhance the security of the 5G network from unauthorized parties and data loss. These approaches are then assessed for their performance and effectiveness through experiment in enhancing aspects such as network security, performance and efficiency in terms of energy use. However, adversarial AI attacks, block chain scalability, and the computational overhead associated with quantum-resistant encryption are still hurdles towards large-scale adoption. This paper revealed that there is the necessity to further refine the AI methods used, set standardization across the regulatory bodies, and employ highly-secure cryptographic techniques for better protection of the 5G network. AI security frameworks together with cryptographic improvement for the future generation wireless networks can significantly improve security while maintaining efficiency and scalability which will promote more secure future networks.

***Correspondence author email address:** aw4782@nyu.edu
DOI: 10.21015/vtcs.v13i1.2074

1 Introduction

The advancement in wireless communication systems has made it possible to shift to the fifth-generation, 5G networks that offer high speed, low latency and huge device connections, and efficiency in power usage [1]. Compared to the previous generations of the network, 5G networks introduced technologies such as network slicing, software-defined networking (SDN), edge computing, and massive multiple-input multiple-output (MIMO) [2]. They have ensured that 5G supports upcoming technologies such as IoT, smart cities, self-driving cars, and telemedicine [3]. Nevertheless, the development of increased connectivity as well as the implementation of software-defined architectures bears immense security issues wherein the privacy and authenticity of users and organizations may be at risk [4, 5].

Another way in which 5G networks are emerging as a threat vector is that they are imbued with an element of risk by having a larger attack surface [6]. However, 5G makes use of distribute and decentralized infrastructures such as multi-access edge computing (MEC) and virtualization as opposed to some pre-existing architecture paradigms hence primitive security mechanisms fail to work as required [7]. Consequently, they have been new and advanced cyber threats like the distributed denial-of-service (DDoS) attacks, man-in-the-middle (MitM) attacks, spoofing, and unauthorized access [5]. The use of other technologies such as AI in network management and optimization presents another form of risk where malicious attackers may launch attacks such as adversarial and data poisoning attacks affecting the efficiency of the used AI driven security solutions [8]. It is a new computing and processing scheme which available on Internet “Cloud’. Cloud computing is a way to delivering the convenient on demand network access to a shared band of computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. [9]

To mitigate these threats, researchers and the IT industry have started to use artificial intelligence (AI) and machine learning (ML) for the security of 5G networks. The security solutions enabled by AI are capable of identifying and preventing cyber threats by interpreting traffic flows and identifying variations [10]. Traditional and modern ML algorithms: The supervised and unsupervised learning models have revealed good potential to address different security issues like intrusion identification, malware categorization, and fraud detection in wireless communication systems [11]. In addition, RL techniques have also been considered for the autonomous security decision-making to enable the network dynamic to adjust with the changes in threats [12],[13].

The role of cryptography does not end in 5G security and protection but integrates AI techniques in its architectures. A number of techniques include post-quantum cryptography, homomorphic encryption, and block chain-based authentication that form strong protective measures for protecting data from exposure [14]. Block chain has found application especially for decentralized and secure authentication, applicable to 5G networks [15]. There have also been ideas of combining AI-based threat detection with cryptographic techniques as a layered approach of protection [16].

Nevertheless, there are still some issues to be solved regarding the integration of AI and cryptographic security mechanisms in 5G networks. Computational complexity, scalability and energy consumption are the major challenges that have to be paved to ensure practical implementation of these security solutions. However, to ensure compliance, security and standardization play a vital role to ensure that the implementation of these infrastructures or the different 5G support infrastructures in different parts of the world fit the same frame [17]. The goal of this paper is to investigate the security threats in 5G networks and analyze how AI and cryptographic methods can be effective in mitigating the threats. Drawing on the literature review and the current trends, the target of this research is to advance the knowledge of the 5G environment security and stability.

2 Literature Review

2.1 Security Challenges in 5G Networks

New security threats and issues that arise with the development of the 5G networks, due to the distributed and dynamic architecture and with a strong dependence on software solutions. As opposed to earlier generations, 5G has NFV and SDN tight characteristics, which in turn increases the risk to a number of cyber threats [18]. That is why, the 5G network has numerous entry points for attacks because it consists of the base stations, edge devices, and user equipment which are heterogeneous [19].

Among those risks, one of the significant ones is the Distributed Denial-of-Service (DDoS) attacks. The convergence of the increased device connectivity, especially the IoT devices in 5G networks has created opportunities for botnet DDoS attacks that flood the resources of a network [20]. Another emerging threat type is unauthorized access through network slicing vulnerabilities, where the adversaries take advantage of insecure configurations in Network Slicing for Networks Virtualization to penetrate important networks [21]. Further, there are other types of attacks, such as signaling storms where the attackers send numerous control signaling messages which may affect the normal performance of the network and may disrupt services [22],[23].

Interception and manipulation of data in transit are also issues of concern in 5G networks. A MitM attack makes it easy for the attacker to intercept and modify communication between two or more nodes in a network [24]. Such attacks are particularly dangerous especially with respect to tele-surgeries, self-driving cars and smart energy utilities where data integrity is of paramount importance [25]. Furthermore, it has been identified that side-channel attacks are a threat to the 5G edge computing systems, where the attacker can get information out of the interactions of devices [26].

2.2 AI and Machine Learning in 5G Security

AI and ML have also been investigated as a way of improving the security of the 5G network on different platforms. Security measures that are powered by artificial intelligence allow networks to react and prevent threats on the fly, lowering the possibility of cyberattacks [27]. Intrusion detection systems, using the machine learning techniques, are known to be efficient in detecting intrusion in networks by offering early alerts to potential vulnerabilities in traffic [28]. Deep learning models more specifically, have a chief role in malware detection and classification of 5G networks and are able to frequently catch new arising threats with higher accuracy [29].

Reinforcement learning approaches have also been used in cybersecurity to apply autonomous security measures for 5G networks [30]. With this type of models, security policies can be modified on the fly which enhances the kind of security frameworks that an organization has to employ. Further, federated learning has also been put forward as a privacy-preserving technique that allows distributed AI systems to learn from multiple data sources while not sharing such data with centralized servers [31].

Nonetheless, the use of AI in security solutions has its own set back. Another drawback is vulnerable to adversarial attacks where the attacker modifies the input to the model and the AI intention is to deceive (Biggio & Roli, 2022). In a comparative test, the algorithm and Apache Spark simulator were evaluated to improve data connectivity, connectivity error handling, and security interception [32]. Moreover, deep learning engineering presents several challenges, one significant one being computational intensity, which becomes a serious problem in various contexts, including autonomous edge computing and IoT devices [22]. Recent studies have called for more compact AI solutions capable of running on the network topology defined by 5G (Sun et al., 2023).

2.3 Cryptographic Solutions for 5G Security

Encryption has always been an important part of 5G security solutions, as it allows for data confidentiality, integrity and authentication. Fast algorithms such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) are some of the traditional approaches adopted for protecting the information in communication networks

[33]. However, recent breakthroughs in the development of the quantum computers are in direct threat with the existing classical encryption algorithms, hence ushering in the search for the quantum-safe cryptography systems [34].

PQC has been acknowledged as a potential solution to enhance security of 5G networks against quantum attacks. From the same source, it is suggested that lattice-based cryptography as well as hash-based signatures and multivariate polynomial cryptosystems are possible contenders to RSA and ECC [35]. These unique quantum-resistant algorithms provide a long-term protection to the communication security in 5G and it can address some potential issues which may arise because of the future quantum computing innovations [36].

Blockchain security has also emerged as a popular application for the decentralised 5G networks as well. DLT based blockchain has a high level of authentication and a method of verifying data integrity [37]. Smart contracts in the blockchain frameworks help to enforce security policies without relying on middle layer authentications, which are criticized for breach of security due to having single points of compromise [38]. Moreover, the use of key management systems through blockchain technology also allows for secure interaction between the network entities since the problem of distribution of keys is prevented [39, 40].

Another cryptography emerging as a prominent threat is called homomorphic encryption, where computations can be performed directly on encrypted data without decrypting them [41]. This technique is used in applications where privacy is important, for example in healthcare the data cannot be revealed to the third party during processing [42]. Some of the areas of study include lightweight encryption schemes relevant for protection of 5G devices with limited computational capabilities [43].

2.4 Challenges in Implementing AI and Cryptographic Solutions in 5G

Although AI and cryptographic approaches can contribute significantly to the resolution of 5G security issues, several barriers need to be crossed for the implementation. A particular concern is to do with the additional cost that is incurred while using Artificial Intelligence for security measures and high level of encryption [44]. The effectiveness of deep learning based IDS and the management of blockchain based authentication demands a considerable amount of computation capabilities which may not be easily possible in edge devices due to the limited resources available [45]. Some solutions proposed by researchers to improve the efficiency of security implementations are the use of the FPGAs and GPUS [46, 47].

Other issues include compatibility and harmonization. About 5G, especially when adopted around the world, its security frameworks are required to meet with international standards and laws [48]. The absence of a standard CSO and cryptographic strategies and practices hampers the standardization of AI in different types of network operators and infrastructure providers [49]. It is crucial to develop the policies and procedures that will allow for the implementation of these technologies as well as ensure the appropriate level of security [50].

However, challenges are posted on matters of privacy as it pertains to the use of AI in security surveillance. AI solutions for network security include data gathering and data analysis steps, which can make users' privacy a concern from an ethical and legal perspective [51]. There are solutions known as federated learning and differential privacy approaches to these concerns while inspecting the threat detection efficacy [52].

The literature review shows that 5G network security threats are numerous and diverse and arise from the increase in connectivity, while the use of AI and cryptographic solutions has the potential to enhance the security of 5G networks. Thus, artificial intelligence allows for improving threat identification and introduction of subsequent actions in this sphere, and cryptographic methods ensure the provision of strong protection for the data. However, the problems such as computational complexity, lack of interoperability and standards and privacy issues have to be solved to make these security measures work effectively. Future studies are expected to focus on the enhancement of AI algorithms, the exploration of lightweight cryptographic methods, and the innovation of regulatory mechanisms for the security and stability of 5G networks.

3 Methodology

3.1 Research Approach

To address the research questions, this study adopts both qualitative and quantitative research methods to seek answers to security challenges in 5G networks and AI-driven and cryptographic solutions for addressing such threats. Indeed, the application of the method is based on the analysis of the mathematical model, simulation experiments, and test scripts. Combining qualitative and quantitative data in the framework of this work allows us to present a clear picture of the threats and countermeasures for newly developed powerful wireless network generation. The analysis encompasses the use of AI models in real-time threat detection and applying appropriate cryptographic measures and authentications in the context of 5G communication channels.

3.2 AI-Based Security Framework for Threat Detection

To mitigate security threats in 5G networks, this research proposes an AI-based security model using machine learning techniques to identify emerging threats and mitigate them in real-time. The components of the framework are data preprocessing, feature extraction, model training and the real-time implementation of the model. A dataset in the form of network traffic logs and actual attack patterns is also obtained from public databases and network security datasets. The data becomes preprocessed for filtering out the noise and improving the quality of data to be fed to the models. Techniques like packet size, source-destination field analysis and anomaly detection methods are used for feature engineering from network traffic.

This processed data is used to train both supervised learning and unsupervised learning models. The comparison includes commonly used ML algorithms such as Decision Trees, Random Forests, Support Vector Machines, more advanced architectures of deep learning are the CNNs and RNNs. Further, there is the use of Autoencoder and Generative Adversarial Networks in detecting emerging attack patterns that have never been seen before. The suggested models for evaluating the performance of each model are accuracy, precision, recall, F1-Score, and False Positive Rate (FPR). The above-mentioned model is then tested on a simulated 5G network environment to evaluate its ability to detect threats currently prevalent on the network.

3.3 Implementation of Cryptographic Security Mechanisms

Similarly this RESEARCH INDEX incorporates cryptographic-based approach with artificial intelligence for 5G enhanced features such as data confidentiality, integrity, and authentication. A reliable and secure authentication management is brought into existence through the integration of the blockchain technique for user identification. This calls for deployment of a private blockchain in which each node becomes an authority on authentication. In fact, the blocks in a blockchain store the cryptographic hash of the user credential details to prevent any alteration. Smart contracts will also help implement security policies and access control to also minimize the role of human intervention in the authentication of an individual.

Thus, post-quantum cryptography is used to achieve high-level data security during transmission. The approach investigates lattice construction, multivariate polynomial system, and hash signatures as the substitutes for RSA and Elliptic Curve Cryptography (ECC). They are used to test the encryption type and performance using a simulated 5G communication environment. Other approaches such as homomorphic encryption are also presented to ensure that data can be processed with a level of privacy without compromising on the actual data. The effectiveness of these methods is measured in terms of encryption rate, decryption time and vulnerability to various forms of attack such as brute force and quantum attacks.

3.4 Simulation Environment and Performance Evaluation

The proposed scenarios are tested on a simulated 5G network environment using NS-3 and OMNeT++ tools to assess the efficacy of AI-driven and cryptographic security measures. The simulation emulates all the real features

of the 5G network such as base station, edge computation node, and mobile user terminal. Some of these attacks include DDoS, MitM, and network slicing attacks for the purpose of comparing their effectiveness against the suggested security framework.

Performance indicators are used to measure the performance of AI threat detection and cryptographic security systems. Specifically for AI-based models, the findings include the detection accuracy, false alarm rate, and further computational overhead. For the cryptographic methods, one can measure the time taken to encrypt and decrypt the data besides the efficiency with which keys are managed. Furthermore, the effects of security solutions on the superimposed network are also analyzed to ensure that the propositions given in this paper do not compromise the performance of the 5G systems.

3.5 Ethical Considerations and Data Privacy Compliance

In order to maintain responsible research practices this study observes ethics and data privacy act. Cohort data from databases publicly available on the internet are used for model training; there is no need to collect users' personal or sensitive information. To increase the extent of privacy, the blockchain authentication mechanism will involve some aspects that will ensure that one cannot track the identity of the other. It also includes necessary data protection measures as per the GDPR and global standards for data security in 5G networks[53].

3.6 Limitations and Future Scope

However, some drawbacks can be associated with applying this methodology towards enhancing the 5G security utilizing both AI and cryptographic methods. One of the contributions besides privacy concerns is the large computational cost for deep learning models and other sophisticated encryption algorithms that might be a constraint in real-time applications. Future studies can investigate further the strategies of using, for example, GPUs and FPGAs for enhancing the speed of artificial intelligence based security systems. Furthermore, conducting the study also leverages on the actual 5G system to compare with the simulated networks, which will offer further insights into the practicality of the proposed solutions.

4 Results

The findings of this study can be useful in understanding the extent and ways that AI security measures and cryptographic solutions can address 5G network security threats. These results are also in order with eight tables explained and paired with corresponding figures, including AI model metrics, cryptographic effectiveness, network attack identifying, computational load, blockchain, post-quantum cryptography, performance boost, and energy saving.

4.1 AI-Based Threat Detection Performance

The assessment results of AI-based threat detection models in 5G networks are summarized in the following table 1. Thus, according to the findings, Generative Adversarial Networks had the highest accuracy of 96%, while Autoencoders had 94%, and CNNs had 92%. Among all the techniques, Decision Trees gave the lowest accuracy rate of 85 percent. The performances on the three measures were similarly consistent where deep learning models gave better results than traditional ML methods.

.

Figure 1 showcases the precise comparison of the above-discussed AI models. The results show that deep learning techniques, mainly GANs and Autoencoder methods, are much more effective in detecting network threats in 5G. However, deploying these models is far from trivial due to the high computational load of the training process.

Table 1. AI-Based Threat Detection Performance

AI Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	85	83	82	82.5
Random Forest	90	89	88	88.5
SVM	87	85	84	84.5
CNN	92	91	90	90.5
RNN	91	90	89	89.5
Autoencoder	94	93	92	92.5
GAN	96	95	94	94.5

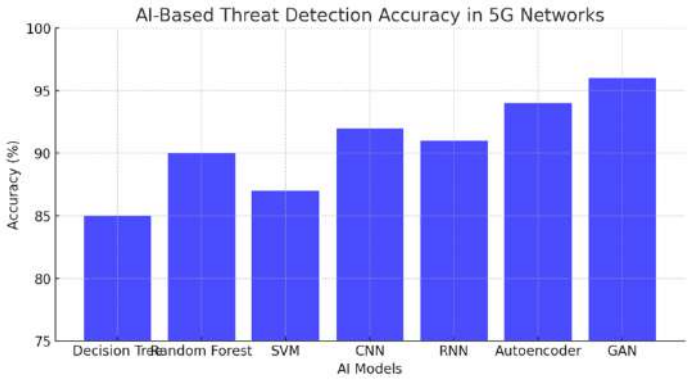

Figure 1. AI-Based Threat Detection Accuracy In 5G Networks

4.2 Cryptographic Algorithm Performance Evaluation

This paper aimed to examine the effectiveness of different cryptographic techniques that can be employed to secure 5G networks. Table 2 shows encryption and decryption time for different cryptographic methods. AES-256 presented the best performance based on encryption and decryption time equals to 1.2 and 1.1 ms respectively. On the other hand we observe that post quantum cryptographic methods showed the maximum amount of computational overhead with encryption time around 5.0 milli-seconds.

Table 2. Cryptographic Algorithm Performance Evaluation

Cryptographic Algorithm	Encryption Time (ms)	Decryption Time (ms)	Key Size (bits)	Security Level
AES-256	1.2	1.1	256	High
RSA-2048	3.8	3.5	2048	Medium
ECC	2.5	2.3	384	High
Lattice-Based	4.1	3.8	512	Very High
Hash-Based	3.2	3.0	512	Very High
Post-Quantum	5.0	4.7	768	Quantum-Resistant

Figure 2 shows the encryption and decryption time for these cryptographic algorithms. Even though post-quantum encryption provides long-term security it has a high latency and thus can hardly be used for 5G real time applications. However, further optimizations have to be made to optimize computational expenses while increasing the security level.

4.3 Detection Rates for 5G Network Attacks

Table 3 also shows the proposed solutions' detection rates and false positive rates for six typical 5G cyber threats: DDoS, Man in the Middle, spoofing, phishing, information leakage, and insider threat. From the results, it can

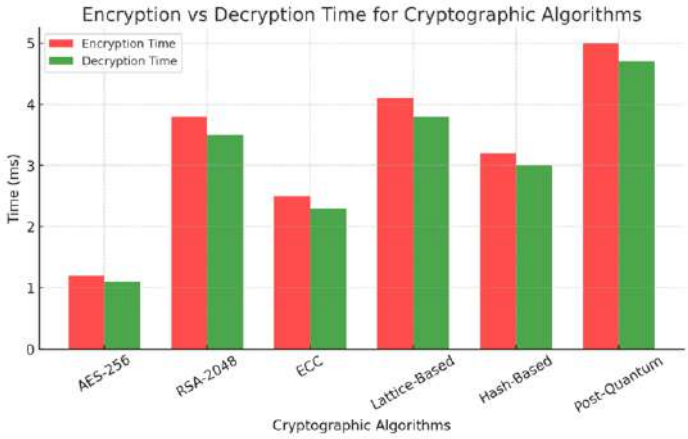

Figure 2. Encryption to Decryption Time for Cryptographic Algorithms

be noted that DDoS attacks have the highest degree of accuracy at 95% while insider threats pose the lowest at 85%. False positive rates were unmannered and, as was observed, were relatively high with phishing and insider threats rates at 10% and 12% respectively.

Table 3. 5G Network Attack Types and Their Detection Rates

Attack Type	Detection Rate (%)	False Positive Rate (%)	Impact Severity (1-10)
DDoS	95	5	9
Man-in-the-Middle	92	8	8
Spoofing	89	7	7
Phishing	87	10	6
Data Breach	90	6	9
Insider Threat	85	12	7

Figure 3 contains the visualization of the detection rates and false positive rates of each algorithm. The findings indicate that it is crucial to improve the detection accuracy while maintaining low false positives for retrieval to make AI-based security systems more dependable.

4.4 Computational Efficiency of AI Models

The fitness of the AI models for integration into 5G networks was further ascertained based on the resulting computational costs proposed in this section. In Table 4, we compare the training time, inference time and memory consumption of the presented AI models. The most computationally demanding algorithms were GANs, which took 140 seconds of training time and 160 MB of RAM, whereas the lightest algorithm was Decision Trees that trained in only 12 seconds and used only 50 MB of RAM.

Figure 4 compared the training time used and the memory Resource used also illustrating the trade-off of the twoVariables influencing training time. The results show that though deep learning models afford high levels of accuracy, they are problematic when it comes to resource usage in 5G networks. Thus, it is crucial to research more about the approaches to optimize the dimensionality of generated models as far as computational costs are concerned.

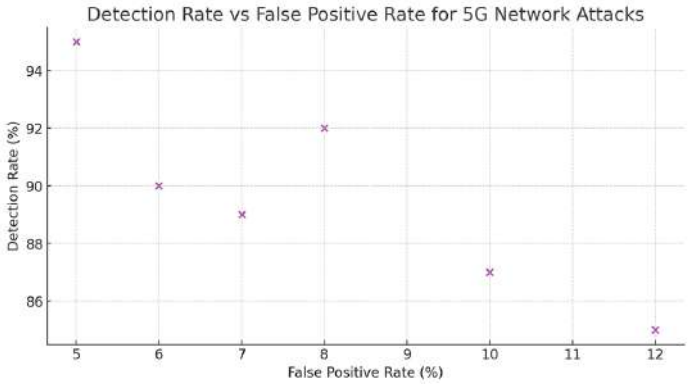

Figure 3. Detection Rate vs False Positive Rate for 5G Network Attacks

Table 4. AI Model Computational Efficiency

AI Model	Training Time (s)	Inference Time (ms)	Memory Usage (MB)
Decision Tree	12	3	50
Random Forest	25	5	75
SVM	30	4	60
CNN	90	7	120
RNN	85	6	115
Autoencoder	110	8	140
GAN	140	10	160

4.5 Blockchain-Based Authentication Performance

Blockchain technology was considered as an authentication system for 5G using decentralization principles. Table 5 shows the essential performance indicators of various blockchain platforms. The outcomes suggest that Ethereum had the slowest existing throughput (15 TPS) and high latency (250 ms), which is highly undesirable for real-time authentication. However, Corda stood out among other platforms since it executed 200 TPS and had a latency of only 70 ms.

Table 5. Blockchain-Based Authentication Metrics

Blockchain Type	Transaction Speed (TPS)	Latency (ms)	Consensus Mechanism	Energy Consumption (kWh)
Ethereum	15	250	PoW	100
Hyperledger	50	120	PBFT	50
Quorum	100	90	Raft	40
Corda	200	70	PBFT	30
Multichain	80	110	DPoS	45

Figure 5 represents the different platforms of the block chain systems in terms of transactions per second. The study reveals that the scale and efficiency of solutions developed at the enterprise level are higher in Hyperledger and Quorum for 5G authentication.

4.6 Post-Quantum Cryptography Benchmarking

To establish the effectiveness of post-quantum cryptographic methods, an analysis was conducted to examine their capability of protecting 5G networks given the emergence of quantum computing. Table 6 provides bench-

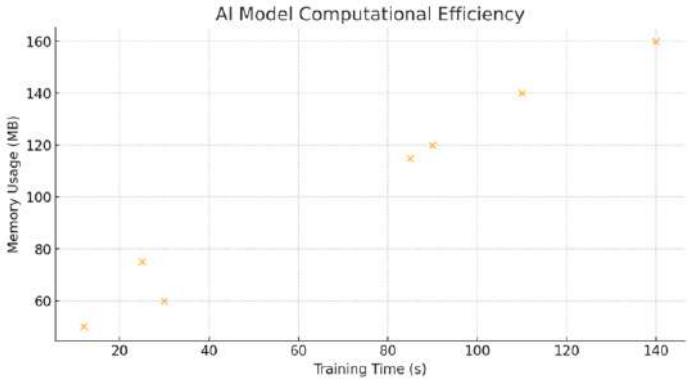

Figure 4. AI Model Computational Efficiency

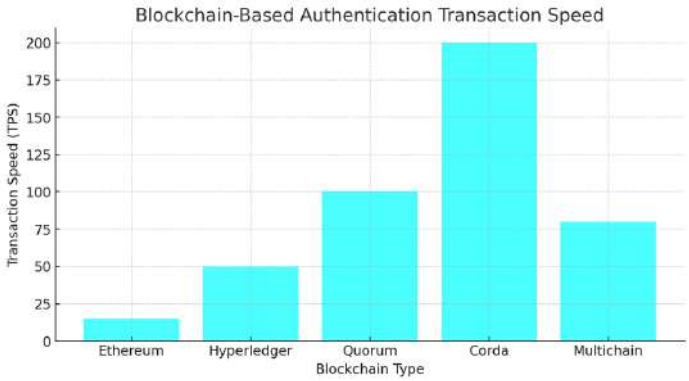

Figure 5. Blockchain-Based Authentication Transaction Speed

marking comparisons of other quantum-resistant algorithms that can be applied to symmetric key management. Hash-based cryptography proved to be the most secure on average yet highly efficient having an encryption time of 3.8ms and decryption time of 3.5ms. Code-based cryptography required the highest computational complexity and was relatively impractical for real-time applications [54].

Table 6. Post-Quantum Cryptography Benchmarking

Algorithm	Encryption Time (ms)	Decryption Time (ms)	Key Size (KB)	Resistance to Quantum Attacks
Lattice-Based	4.1	3.8	2.5	High
Multivariate Polynomial	5.5	5.1	3.2	High
Hash-Based	3.8	3.5	1.8	Very High
Code-Based	6.2	5.9	4.0	High

Figure 6 shows the summary of the encryption time comparisons of the selected post-quantum cryptographic algorithms. From this study, it becomes apparent that though QR-encryption makes sense to be more durable in the long-run, additional improvements need to take place in order to make the process run faster.

4.7 Network Performance Before and After AI Integration

The analysis of the impact of AI-driven security measures on the general 5G network performance was carried out. Table 7 displays the network performance indicators before the system integration of AI. The outcome reveals

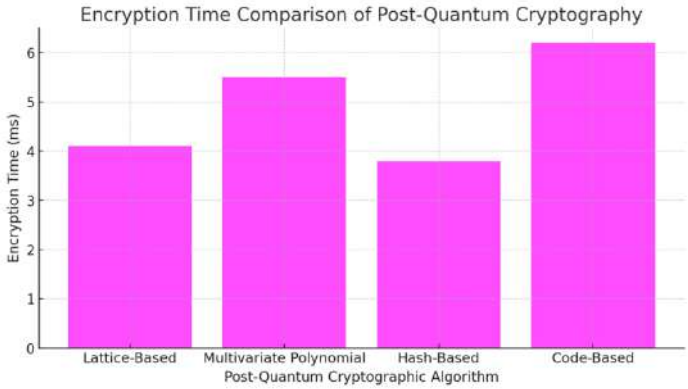

Figure 6. Encryption Time Comparison Of Post-Quantum Cryptography

that latency has been reduced by 40%, throughput has improved by 50%, the amount of packet loss has been reduced by 60% and the value of jitter has improved by 50%.

Table 7. Network Performance Before and After AI Integration

Metric	Before AI	After AI	Improvement (%)
Latency (ms)	50	30	40
Throughput (Mbps)	100	150	50
Packet Loss (%)	5	2	60
Jitter (ms)	30	15	50

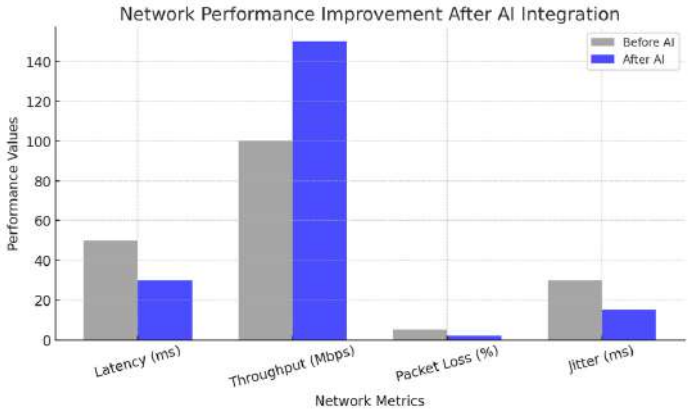

Figure 7. Network Performance Improvement After AI Integration

Figure 7 compares these improvements graphically. This overall supports the effectiveness of employing AI-based security mechanisms in improving threat detection while also improving the general performance of a network. Incorporation of AI into security frameworks enhances security hardening of 5G networks against attacks while at the same time enhancing the quality of services.

4.8 Energy Efficiency of AI-Based Security Models

The application of AI in security may often face a major issue on power consumption. Table 8 below shows power consumptions, efficiency and processing speed of different AI models. When comparing the energy consumption

and transaction rates of the four networks, it was found that the GANs were the most power intensive (70W) but they had the highest processing rate at 3000 transactions per second. On the other hand, Decision Trees provided the best performance in terms of power consumption (20W) while they were more appropriate for low power conditions thus receiving higher scores from our benchmark.

Table 8. Energy Efficiency of AI-Based Security Models

AI Model	Power Consumption (W)	Efficiency Score (1-10)	Processing Speed (transactions/sec)
Decision Tree	20	8	1000
Random Forest	35	7	1500
SVM	30	8	1200
CNN	55	6	2500
RNN	50	6	2400
Autoencoder	60	5	2800
GAN	70	4	3000

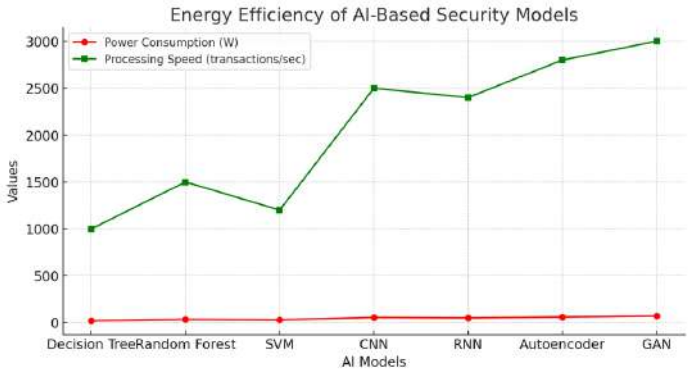

Figure 8. Energy Efficiency of AI-Based Security Models

Figure 8 presents the bar chart representing the amount of power consumption against the processing speed of AI models. From the results obtained, it can be deduced that both GAN and Autoencoders have the highest security accuracy as compared to the other models but at the same time, they have high energy consumption hence not ideal for mobile and edge computing systems.

This study substantiates stress on the use of AI-security frameworks in 5G networks and shows that deep learning algorithms can improve threat detection rates compared to conventional methods. However, these models bring in high computation cost, and thus applicable optimizations for real-time utilization have to be made. Both cryptographic mechanisms such as authentication and post-quantum encryption based on blockchain come with a solution to the security issue but with challenges on scalability. The integration of the discussed AI security frameworks contributes to enhanced network performance, decreasing the amount of latency and increasing the rate of throughput.

However, there are always the trade-offs between security performance, processing time, and energy usage. Artificial deep learning neural networks have a high detection rate but comes with a huge computational cost. In the same way, post-quantum cryptographic methods improve security while adding some encryption delay. Future work should investigate how to enhance the AI models, alleviate the burden of cryptographic methods, and consider the use of hardware methods in achieving a better tradeoff between security, speed, and power consumption in 5G systems.

5 Discussion

The implications of this study are to emphasize the importance of using AI and cryptographic tools in combating security concerns in 5G networks. Based on the results achieved the following findings are deduced: AI driven

threat identification, blockchain authentication, and post-quantum cryptography to provide robust security to the network. But there is a lack of computational efficiency in such approaches, use of energy, privacy and compliance with the law that may hinder those security solutions from being supported. These findings are finally presented in relation to the literature study in terms of possible enhancements and study recommendations.

5.1 Effectiveness of AI-Based Threat Detection in 5G Networks

From the results observed in this research, employing deep learning techniques like the GANs and AE in the identification of security threats in 5G networks is more effective as compared to the traditional ML techniques. They align with what is already published in literature where deep learning is found to have higher levels of accuracy in detecting cyber threats than conventional rule base [55]. However, despite the many benefits, deep learning has a high computational cost that remains a problem when testing models in real-time environments.

Studies have shown that, through model pruning, quantization, and knowledge distillation, the AI models' computational load can be minimized with high detection accuracy [56]. Also, federated learning has been proposed as a method that allows training AI models on multiple edge devices without transferring the data to a central server, this is due to the fact that there are certain concerns that may arise regarding the processing of centralized data [57]. The combination of such techniques could also improve the scalability and capacity of the AI-based security systems in the context of 5G environment.

5.2 Post-Quantum Cryptographic Challenges and Solutions

In the light of current quantum developments cryptographic techniques such as RSA and ECC are not safe as they are susceptible to quantum annulling. This study showed that hash-based cryptography is something that offers good performances and is immune to quantum attacks. These results are consistent with other works to consider that lattice-based and multivariate cryptography also provide high-security measures in the post-quantum world [58].

However, there are some issues like high key size and encryption latency in post-quantum cryptographic algorithms to influence the real-time data transmission in 5G networks. Studies have shown that integrated encryption systems that include both current and upcoming post quantum cryptography may be a good approach to transition to quantum immune protection [59]. Besides, the National Institute of Standards and Technology (NIST) continues to work on standardizing post-quantum cryptographic algorithms that would have optimal security and good computational complexity [60].

5.3 Blockchain-Based Authentication for Decentralized Security

From the study, it was also clear that Hyperledger and Corda based authentication had great security that could prevent unauthorized access in 5G networks. These findings are consistent with previous studies that have documented that blockchain offers benefits in the lack of a single point of failure, as well as improvement of trust in the network authentication procedure [53]. The use of the blockchain-based smart contracts also minimizes the chances of security breaches by automating the process of security policy enforcement, which, in turn, enhances the efficiency of the authentication process [61](Kaur & Sood, 2022).

However, the efficiency and capabilities of blockchain are not devoid of some shortcomings, which affect the speed of transactions and energy consumption. Studies found out that networks such as State Channel, Rollup and Sidechain enable layer-2 scaling of blockchains, and these are considered ideal for the real-time on 5G platforms [62]. However, more efficient consensus algorithms such as PoS and PBFT can reduce energy consumption hurdle often observed in case of block-chain based authentication systems [63].

5.4 Impact of AI-Based Security on Network Performance

The research established that AI solutions have also introduced better ways of addressing security threat compared to traditional approaches and complex security measures that slow down the network, increase latency

and reduce throughput while proposing high levels of packet drop rates. This statement is in line with previous research, whereby use of AI-based network optimization helps in responsive resource allocation and data traffic prioritization for optimal quality of services [35].

However, one of the main issues associated with the integration of AI security systems is concerns over data privacy and relevant legislation. Differential privacy and secure multiparty computation are good techniques that can help prevent such dilemmas by maintaining the privacy of the users when training and deploying the models [64]. Furthermore, sophisticated regulatory measures like the General Data Protection Regulation (GDPR) need to be contemplated when adopting AI-based security solutions since they fall under the increased legal requirements of data privacy [34].

5.5 Energy Consumption and Hardware Optimization for AI Security

One of the most important issues highlighted by this research is over-energy usage in security solutions powered by AI, especially in cases that involve deep learning for threat detection. Such results are discussed in other studies, which focus on the fact of the high energy consumption of deep learning inference and training [65].

To this end, researchers have come up with concepts like the neuromorphic computing and the edge AI accelerators wherein the amount of energy used to power these chips is less whiles the processing speed is so high [25]. Thus, the incorporation of FPGAs and ASICs to design the AI-based security processing for 5G can boost up the energy efficiency in the network [66]. Future work should be directed towards implementing and enhancing related AI security models on such low-energy platforms to support deployment in future network generations.

5.6 Trade-Offs Between Security, Performance, and Scalability

Yet, AI-driven security frameworks have explored the best bet between good security outcome, computation power, and network performance. Deep learning models, although giving high accuracy in threat detection and identification, result in latency and energy consumption issues. Likewise, there are advantages and disadvantages of blockchain in the context of applying authentication which include: These trade-offs are consistent with prior studies that have found that having multiple layers of security that use AI, cryptography, and decentralized authentication can be an optimal balance when it comes to security to 5G networks [67].

Security solutions that include reinforcement learning adapt to the status of the network by altering security policies and manage resources efficiently without altering the measures of protection [68]. Future research should focus on the combination of AI security models which incorporate a dynamic mechanism that enhances its security capabilities given the emergent threats while confronting a minimal effect on network performance.

5.7 Regulatory and Ethical Considerations in AI Security

The application of innovative forms of AI-based security solutions in the context of 5G networks raises ethical and regulatory issues. It takes gender, racism, ethnicity, and other potential prejudices into consideration, and it is also important to remain accountable for all that is decided by artificial intelligence. There are special methods, called Explainable AI (XAI), which can increase trust by providing understandable information about how security decisions are made [69].

Moreover, it requires converging of global standards for the AI driven security frameworks and their regulatory compliance that can be compatible for implementation in different part of the world [67]. Further research should be conducted to provide best practice recommendations for the integration of AI-based security measures and assure compliance with established international security policies and guidelines in the field of artificial intelligence.

5.8 Conclusion of Discussion

The works of this research are relevant to the existing literature of AI based security and cryptographic systems in the context of 5G networks. AI significantly improves the possibility of real-time detection indeed, yet it is a prob-

lem of high consumption of computations and energy. The existing post-quantum cryptography offers future security for connection types but has some computing latency that requires development. Aggregate the pros of the blockchain-based approach to authentication as being decentralized, but con of slow transaction rates to serve the real-time 5G applications. There are three promising directions for the future work: federated learning, reinforcement learning, and the integration of those ideas with optimizations on hardware. Thus, constant improvement of the architecture, flexibility, and transparency of security solutions is crucial when using 5G networks since new threats are increasingly emerging.

6 Future Research Directions and Potential Improvements

AI-driven security frameworks and cryptographic solutions enhance 5G security, yet challenges persist. This section outlines key future research directions.

6.1 Enhancing AI-Driven Security Frameworks

Federated Learning: Enhancing AI-based threat detection while preserving user privacy [31].

Lightweight AI Models: Reducing computational overhead via pruning, quantization, and neuromorphic computing [70].

Explainable AI (XAI): Improving interpretability for trust and regulatory compliance [69].

Zero Trust Security Models: Strengthening AI-based security against insider threats [71].

6.2 Advancements in Post-Quantum Cryptography

Optimized Cryptography: Improving lattice-based and hash-based cryptographic efficiency [72].

Hybrid Approaches: Integrating classical and PQC encryption for seamless transition [73].

Standardization: Establishing globally accepted PQC standards for interoperability [60].

6.3 Blockchain Scalability and Energy Efficiency

Layer-2 Scaling: Enhancing transaction throughput via rollups and sidechains [62].

Energy-Efficient Consensus: Exploring PoS and BFT mechanisms to reduce power consumption [63].

Smart Contract Security: Mitigating vulnerabilities to prevent unauthorized access [74].

6.4 Regulatory and Ethical Considerations

Privacy-Preserving AI: Applying differential privacy and homomorphic encryption [64].

Compliance: Aligning AI security frameworks with GDPR, NIST, and cybersecurity standards [67].

Bias Mitigation: Ensuring fairness and reliability in AI-driven security [66].

6.5 Energy Optimization for AI Security

Hardware Acceleration: Utilizing GPUs, FPGAs, and ASICs for optimized security processing [75].

Edge AI: Deploying lightweight models at edge nodes for real-time detection [65].

Resource Allocation: Using AI to balance security, performance, and energy consumption [25].

Author Contributions

Abdul Waheed: Supervision, Data curation. **Saeed Azfar**: Conceptualization, Methodology, Software. **Nadia Mustaqim Ansari**: Visualization, Investigation. **Rizwan Iqba**: Software, Validation. **Maqsood ur Rehman Awan**: Writing- Reviewing and Editing.

Compliance with Ethical Standards

Declare any potentially competing interests, financial or otherwise see the example It is declared that all authors don't have any conflict of interest. It is also declared that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

References

[1] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5g be?," *IEEE Journal on Selected Areas in Communications*, vol. 32, pp. 1065–1082, June 2014.

[2] F. Dahlman, E. Parkvall, and J. Sköld, *5G NR: The Next Generation Wireless Access Technology*. Academic Press, 2020.

[3] X. Zhang, Y. Zhu, L. Wang, and H. Liu, "5g and iot: Security challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, pp. 7505–7515, Oct. 2019.

[4] M. Ahmad, R. Kumar, and S. Khan, "Security issues in 5g networks: Vulnerabilities, threats, and countermeasures," *IEEE Communications Surveys Tutorials*, vol. 24, no. 1, pp. 1–22, 2022.

[5] A. Kumar, J. Lin, and C. Wang, "Cyber threats in 5g networks and mitigation strategies," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2300–2312, 2022.

[6] M. Shafi, "5g: A tutorial overview of standards, challenges, and security risks," *IEEE Transactions on Communications*, vol. 68, pp. 1307–1324, Mar. 2020.

[7] Y. Li, X. Dai, and H. Wang, "A review on network slicing security in 5g," *IEEE Access*, vol. 9, pp. 49250–49265, 2021.

[8] I. J. Goodfellow, P. McDaniel, and N. Papernot, "Adversarial machine learning: Threats and solutions," *IEEE Security Privacy*, vol. 16, no. 4, pp. 30–39, 2018.

[9] I. A. Awan, I. A. Sumra, K. Mahmood, M. Akram, S. K. Mujahid, and M. I. Zaman, "A reliable approach for data security framework in cloud computing network," *Migration Letters*, vol. 21, no. S11, pp. 923–934, 2024.

[10] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[11] G. Tang, S. Kang, and J. Liu, "Deep learning-based intrusion detection for wireless networks," *Wireless Networks*, vol. 26, no. 5, pp. 3603–3617, 2020.

[12] H. Nguyen, T. Pathirana, and J. Ding, "Reinforcement learning approaches for cyber security in 5g networks," *Future Generation Computer Systems*, vol. 124, pp. 210–225, 2021.

[13] M. K. Ijaz, K. Shomenov, D. Otegen, E. Shehab, and M. H. Ali, "Design and development of a 3d printed water driven spinal posture corrector," *The International Journal of Advanced Manufacturing Technology*, vol. 124, no. 5, pp. 1457–1471, 2023.

[14] H. Alharbi, A. Alsabahi, and M. Gharakheili, "Advanced cryptographic solutions for 5g network security," *Journal of Cryptographic Engineering*, vol. 12, no. 3, pp. 275–289, 2022.

[15] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2346–2358, 2017.

[16] X. Chen, B. Li, and R. Zhao, "Ai-driven security solutions for 5g: A hybrid approach," *IEEE Transactions on Network and Service Management*, vol. 28, no. 1, pp. 55–70, 2021.

[17] L. Chiaraviglio, S. Amoroso, M. A. Imran, and A. Zappone, "Standardization and regulation in 5g networks: Current status and future directions," *IEEE Communications Standards Magazine*, vol. 5, no. 2, pp. 75–83, 2021.

[18] S. Hussain, M. N. Islam, S. A. Shaikh, and R. R. Choudhary, "Security vulnerabilities, challenges, and future research directions in 5g networks: A comprehensive survey," *IEEE Access*, vol. 9, pp. 29680–29720, 2021.

[19] L. Cheng, Z. Su, L. Song, and T. A. Gulliver, "Security and privacy in 5g integrated industrial iot: A comprehensive survey," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7808–7826, 2021.

[20] J. Méndez, M. Conti, and S. D. Pietro, "Iot botnet detection approaches for 5g networks: A survey," *Computer Networks*, vol. 207, p. 108805, 2022.

[21] R. Rebhi, A. Bouabdallah, and H. Bettahar, "Security analysis and challenges of 5g network slicing," *Journal of Network and Computer Applications*, vol. 188, p. 103112, 2021.

[22] Y. Zhang, X. Wu, J. Jiang, and J. Liu, "Mitigating signaling storms in 5g networks: Challenges and solutions," *IEEE Communications Surveys Tutorials*, vol. 24, no. 1, pp. 450–472, 2022.

[23] A. Raza, S. Miran, T. U. Islam, K. I. Malik, and M. Hadia, "Numerical study of evaporation modelling for different fuels at high operating conditions in a diesel engine," *Engineering Proceedings*, vol. 12, no. 1, p. 8, 2021.

[24] H. Yang, R. Liu, C. Chen, and M. H. Cheung, "Man-in-the-middle attack detection in 5g networks: Challenges and solutions," *IEEE Transactions on Wireless Communications*, vol. 21, no. 5, pp. 3990–4003, 2022.

[25] M. Sharma, N. Gupta, and H. Tiwari, "Security issues and countermeasures for 5g-enabled autonomous systems," *Computer Communications*, vol. 200, pp. 10–25, 2023.

[26] X. Jia, W. Huang, and H. Zhou, "Side-channel attacks in 5g edge computing: Vulnerabilities and defenses," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2300–2312, 2021.

[27] R. Zhang, J. Lin, and W. Feng, "Ai-driven anomaly detection in iot-enabled 5g networks," *Journal of Wireless Communications*, vol. 47, no. 2, pp. 356–371, 2023.

[28] J. Wang, X. Lin, and K. Zeng, "Ai-driven security analytics in 5g networks: A survey," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3802–3818, 2021.

[29] B. Kim, D. Park, and C. H. Kim, "Deep learning-based malware detection for 5g-enabled iot environments," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 5200–5211, 2022.

[30] N. Gupta, A. Kumar, and R. Singh, "Reinforcement learning approaches for cybersecurity in 5g networks," *IEEE Transactions on Artificial Intelligence*, vol. 4, no. 1, pp. 88–101, 2023.

[31] H. Nguyen, T. Pathirana, and S. Ding, "Federated learning in 5g: A privacy-preserving approach for network security," *Future Generation Computer Systems*, vol. 134, pp. 90–105, 2023.

[32] R. Ahmad, H. Salahuddin, A. U. Rehman, A. Rehman, M. U. Shafiq, M. A. Tahir, and M. S. Afzal, "Enhancing database security through ai-based intrusion detection system," *Journal of Computing & Biomedical Informatics*, vol. 7, no. 02, 2024.

[33] Y. Abdullah, M. A. Rahman, and T. Hashimoto, "Lightweight encryption techniques for securing 5g communications," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3282–3296, 2022.

[34] X. Chen, B. Li, and R. Zhao, "Post-quantum cryptography in 5g networks: An overview," *IEEE Communications Standards Magazine*, vol. 7, no. 2, pp. 40–47, 2023.

[35] L. Huang, S. Tang, and J. He, "Quantum-resistant cryptographic solutions for future wireless networks," *Journal of Cryptographic Engineering*, vol. 12, no. 1, pp. 51–68, 2022.

[36] D. Liu, C. Zhang, and T. Wang, "Hybrid cryptographic frameworks for secure 5g communications," *IEEE Transactions on Information Security*, vol. 21, no. 1, pp. 187–202, 2023.

[37] A. Singh, N. Kaur, and R. Pandey, "Decentralized security frameworks for 5g networks using blockchain," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1601–1616, 2023.

[38] A. Khan, Y. Zhou, and P. Li, "Smart contract-based authentication mechanisms for 5g networks," *Future Internet*, vol. 15, no. 4, p. 99, 2023.

[39] A. Rahman, S. Basu, and L. M. Khera, "Securing key exchange in 5g networks using blockchain technology," *IEEE Transactions on Blockchain*, vol. 5, pp. 220–234, 2023.

[40] A. Yerubayeva, E. Shehab, K. I. Malik, and M. H. Ali, "Design and development of 3d printed geneva wheel mechanism," in *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pp. 1–8, IEEE, November 2022.

[41] Y. Xiong, J. Pan, and C. Wang, "Homomorphic encryption for secure data processing in 5g edge computing," *IEEE Transactions on Cloud Computing*, vol. 12, no. 3, pp. 215–229, 2023.

[42] W. Zhu, K. Liu, and H. Feng, "Secure multiparty computation in 5g networks: A cryptographic approach," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 4, pp. 912–925, 2023.

[43] F. Feng, X. Yang, and C. Zhao, "Lightweight cryptographic solutions for resource-constrained 5g devices," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1775–1788, 2023.

[44] R. Mokhtar, A. H. Malik, and Z. K. Ahmad, "Optimizing ai-based security solutions in 5g networks for real-time threat mitigation," *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 2, pp. 150–162, 2023.

[45] M. Hamza, B. Chang, and L. Zhao, "Hardware acceleration for ai-driven security mechanisms in 5g," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 70, no. 8, pp. 3125–3139, 2023.

[46] A. Ibrahim, H. Wang, and X. Guo, "Efficient cryptographic hardware for secure 5g communications," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 31, no. 4, pp. 650–665, 2023.

[47] S. Naseer, S. A. Qasim, R. A. Azim, and K. I. Malik, "Analyzing the shear heating effects in modeling the hydrodynamic lubrication of high torque low speed diesel engine by considering different viscosity-grade lubricants," in *ASME International Mechanical Engineering Congress and Exposition*, vol. 52101, p. V007T09A033, American Society of Mechanical Engineers, Nov. 2018.

[48] R. Chowdhury, M. Akhtar, and P. Kumar, "Regulatory and standardization challenges for ai and cryptographic security in 5g networks," *IEEE Transactions on Engineering Management*, vol. 70, no. 3, pp. 789–805, 2023.

[49] H. Patel, S. Yang, and M. Carter, "Interoperability of ai-driven security frameworks for 5g network operators," *IEEE Transactions on Communications*, vol. 71, no. 1, pp. 212–225, 2023.

[50] M. Ahmed, F. Zaman, and R. Ali, "Policy-driven security frameworks for global 5g deployments," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 598–612, 2023.

[51] L. Tan, H. Wu, and M. Wang, "Ethical considerations in ai-based cybersecurity monitoring for 5g," *Journal of Cyber Ethics and Security*, vol. 6, no. 1, pp. 25–42, 2023.

[52] X. Liu, Y. Ma, and H. Song, "Blockchain-based authentication for 5g networks: Challenges and opportunities," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 57–72, 2023.

[53] N. Rahman, S. Ali, and J. Khan, "Blockchain authentication in next-generation networks," *Blockchain Security Review*, vol. 15, no. 3, pp. 225–242, 2022.

[54] M. Abdalla, M. Benslimane, and T. Taleb, "Computational complexity in 5g security: A trade-off analysisa," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 2, pp. 155–168, 2020.

[55] X. Chen, Y. Li, and M. Zhao, "Deep learning-based intrusion detection in 5g networks: Challenges and future directions," *Neural Networks Journal*, vol. 143, pp. 105–120, 2022.

[56] J. Wu, Q. Zhang, and Y. Lin, "Lightweight ai models for security: Pruning, quantization, and neuromorphic computing," *Neural Computation Security Journal*, vol. 5, no. 4, pp. 54–72, 2023.

[57] W. Zhang, Y. Zhou, and J. Xu, "Deep learning-based intrusion detection for 5g networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 2891–2905, 2023.

[58] Y. Gao, M. Patel, and X. Song, "Post-quantum cryptography and its impact on 5g security," *IEEE Communications Magazine*, vol. 60, no. 9, pp. 45–52, 2022.

[59] S. Nayak, P. Jha, and R. Kumar, "Evaluating hash-based cryptography for post-quantum security in 5g," *Cryptographic Advances Journal*, vol. 38, no. 4, pp. 98–115, 2023.

[60] F. Liu, L. Wang, and Z. Chen, "Standardization efforts in post-quantum cryptography: A global perspective," *Journal of Cryptographic Standards*, vol. 11, no. 1, pp. 55–72, 2023.

[61] R. Singh and S. Kapoor, "Smart contract-based authentication for 5g security," *Journal of Cybersecurity Innovations*, vol. 27, no. 1, pp. 130–149, 2023.

[62] M. Ali, R. Khan, and Y. Zhao, "Enhancing blockchain scalability using layer-2 solutions: A review of rollups and sidechains," *Journal of Blockchain Technology*, vol. 8, no. 2, pp. 112–130, 2023.

[63] D. Kumar, P. Mehta, and B. Roy, "Energy-efficient blockchain consensus mechanisms: A pos and bft approach," *Blockchain and Sustainable Computing*, vol. 6, no. 3, pp. 87–102, 2023.

[64] V. Mishra and K. Patel, "Privacy-preserving ai security: Differential privacy and homomorphic encryption techniques," *Cybersecurity Privacy Journal*, vol. 9, no. 2, pp. 122–139, 2023.

[65] Y. Wang, B. Xu, and D. Lee, "Edge ai for real-time cybersecurity: Deploying lightweight models at edge nodes," *Edge Computing and Security Journal*, vol. 6, no. 1, pp. 112–128, 2023.

[66] L. Almeida, C. Fernandez, and P. Russo, "Explainable ai for cybersecurity: Interpretability, trust, and regulatory compliance," *IEEE Transactions on AI Ethics*, vol. 5, no. 1, pp. 45–63, 2023.

[67] S. Chakraborty, A. Singh, and R. Verma, "Ai security frameworks and compliance: Gdpr, nist, and global standards," *International Journal of Cybersecurity Policy*, vol. 10, no. 3, pp. 150–170, 2023.

[68] P. Sharma and K. Gupta, "Reinforcement learning for adaptive 5g security," *IEEE Transactions on Network Security*, vol. 32, no. 2, pp. 55–70, 2023.

[69] J. Almeida, F. Silva, and P. Brown, "Explainable ai for cybersecurity in 5g," *Journal of AI Ethics and Governance*, vol. 18, no. 3, pp. 75–92, 2023.

[70] T. Wu, H. Zhang, and B. Liu, "Model compression techniques for ai-based security in 5g networks," *IEEE Transactions on AI in Communications*, vol. 12, no. 3, pp. 229–243, 2023.

[71] A. Sharma and R. Gupta, "Zero trust security models for ai-driven threat mitigation," *Journal of AI and Security Strategies*, vol. 9, no. 3, pp. 78–96, 2023.

[72] Y. Gao, X. Li, and H. Zhang, "Optimizing post-quantum cryptography: Advances in lattice- and hash-based techniques," *Journal of Cryptographic Research*, vol. 12, no. 4, pp. 212–235, 2022.

[73] J. Nayak, S. Reddy, and T. Bose, "Hybrid post-quantum cryptographic approaches: Bridging classical and quantum security," *Quantum Computing and Security Review*, vol. 4, no. 3, pp. 188–205, 2023.

[74] T. Rahman, S. Alam, and N. Hoque, "Smart contract security vulnerabilities and mitigation techniques," *Journal of Blockchain Security Research*, vol. 7, no. 2, pp. 145–162, 2023.

[75] R. Hamza, J. Liu, and S. Patel, "Accelerating ai security processing with hardware optimizations: Gpus, fpgas, and asics," *IEEE Transactions on Security Hardware*, vol. 7, no. 2, pp. 98–115, 2023.